

日 本 国 特 許 庁
JAPAN PATENT OFFICE

18.10.2004

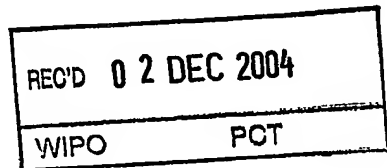
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 1 0 月 1 6 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 3 5 6 0 7 3
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 3 5 6 0 7 3]

出 願 人 松下電器産業株式会社
Applicant(s):

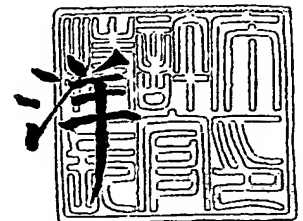


PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2 0 0 4 年 1 1 月 1 8 日

特許庁長官
Commissioner,
Japan Patent Office

小 川



BEST AVAILABLE COPY

【書類名】 特許願
【整理番号】 2022550348
【提出日】 平成15年10月16日
【あて先】 特許庁長官殿
【国際特許分類】 G09C 5/00
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 布田 裕一
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 山道 将人
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 大森 基司
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 館林 誠
【特許出願人】
 【識別番号】 000005821
 【氏名又は名称】 松下電器産業株式会社
【代理人】
 【識別番号】 100097445
 【弁理士】
 【氏名又は名称】 岩橋 文雄
【選任した代理人】
 【識別番号】 100103355
 【弁理士】
 【氏名又は名称】 坂口 智康
【選任した代理人】
 【識別番号】 100109667
 【弁理士】
 【氏名又は名称】 内藤 浩樹
【手数料の表示】
 【予納台帳番号】 011305
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9809938

【書類名】 特許請求の範囲**【請求項 1】**

第 1 の機器と第 2 の機器を備え、前記第 1 の機器と前記第 2 の機器との間で鍵配送を行い、共有した鍵を用いて前記第 1 の機器から前記第 2 の機器へコンテンツデータを送信する暗号通信システムであって、

前記第 1 の機器は、

第 1 の公開鍵証明書と第 1 のコンテンツデータを格納する第 1 のデータ格納部と、

前記第 2 の機器へデータを送信する第 1 の送信部と、

前記第 2 の機器から送信されたデータを受信する第 1 の受信部と、

第 2 の公開鍵証明書を検証する第 1 の証明書検証部と、

第 1 の鍵と第 1 の鍵を暗号化した第 1 の暗号化鍵を生成する第 1 の暗号化鍵生成部と、

第 2 の暗号化鍵から復号化し、復号化した結果を第 2 の鍵として出力する第 1 の暗号化鍵復号部と、

前記第 1 の鍵と前記第 2 の鍵に基づき共有鍵を生成する共有鍵生成部と、

前記共有鍵を格納する共有鍵格納部と、

前記共有鍵の一部または全部を用いて、前記第 1 のコンテンツデータを共通鍵暗号を用いて暗号化した第 1 の暗号化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて第 1 のハッシュ値を生成する第 1 の暗号化部とを含み、

前記第 2 の機器は、

前記第 2 の公開鍵証明書と前記第 2 のコンテンツデータを格納する第 2 のデータ格納部と、

前記第 1 の機器へデータを送信する第 2 の送信部と、

前記第 1 の機器から送信されたデータを受信する第 2 の受信部と、

前記第 1 の公開鍵証明書を検証する第 2 の証明書検証部と、

第 2 の鍵と第 2 の鍵を暗号化した前記第 2 の暗号化鍵を生成する第 2 の暗号化鍵生成部と、

前記第 1 の暗号化鍵から復号化し、復号化した結果を前記第 1 の鍵として出力する第 2 の暗号化鍵復号部と、

前記第 1 の鍵と前記第 2 の鍵に基づき共有鍵を生成する前記共有鍵生成部と、

前記共有鍵を格納する前記共有鍵格納部と、

前記第 1 の暗号化コンテンツデータを復号化し、第 1 の復号コンテンツデータを取得し、前記第 1 の復号コンテンツデータに対して、前記共有鍵の一部または全部と前記鍵付ハッシュ関数を用いて第 2 のハッシュ値を生成し、前記第 1 のハッシュ値と比較する第 1 の復号化部とを含むこと

を特徴とする暗号通信システム。

【請求項 2】

第 1 の機器はさらに、第 2 の暗号化コンテンツデータを復号化し、第 2 の復号コンテンツデータを取得し、前記第 2 の復号コンテンツデータに対して、前記共有鍵の一部または全部と前記鍵付ハッシュ関数を用いて第 3 のハッシュ値を生成し、第 4 のハッシュ値と比較する第 2 の復号化部を含み、

第 2 の機器はさらに、前記共有鍵の一部または全部を用いて、前記第 2 のコンテンツデータを暗号化した前記第 2 の暗号化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて前記第 4 のハッシュ値を生成する第 2 の暗号化部を含むこと

を特徴とする請求項 1 記載の暗号通信システム。

【請求項 3】

前記第 1 の暗号化鍵及び前記第 2 の暗号化鍵は、鍵カプセル化メカニズムを用いて生成すること

を特徴とする請求項 1 または請求項 2 記載の暗号通信システム。

【請求項 4】

前記共有鍵生成部は、前記第 1 の鍵と前記第 2 の鍵の排他的論理和を前記共有鍵として出

力すること

を特徴とする請求項 1 から請求項 3 のいずれか 1 項に記載の暗号通信システム。

【請求項 5】

前記共有鍵生成部は、前記第 1 の鍵と前記第 2 の鍵をビット連結したものをハッシュ関数を用いて計算したハッシュ値を前記共有鍵として出力すること

を特徴とする請求項 1 から請求項 3 のいずれか 1 項に記載の暗号通信システム。

【請求項 6】

第 1 の機器と第 2 の機器を備え、前記第 1 の機器と前記第 2 の機器との間で鍵配送を行う認証鍵共有システムであって、

前記第 1 の機器は、

第 1 の公開鍵証明書と第 1 のコンテンツデータを格納する第 1 のデータ格納部と、

前記第 2 の機器へデータを送信する第 1 の送信部と、

前記第 2 の機器から送信されたデータを受信する第 1 の受信部と、

第 2 の公開鍵証明書を検証する第 1 の証明書検証部と、

鍵カプセル化メカニズムを用いて第 1 の鍵と第 1 の鍵を暗号化した第 1 の暗号化鍵を生成する第 1 の暗号化鍵生成部と、

第 2 の暗号化鍵から復号化し、第 2 の鍵を出力する第 1 の暗号化鍵復号部と、

前記第 1 の鍵と前記第 2 の鍵に基づき共有鍵を生成する共有鍵生成部と、

前記共有鍵を格納する共有鍵格納部とを含み、

前記第 2 の機器は、

前記第 2 の公開鍵証明書と前記第 2 のコンテンツデータを格納する第 2 のデータ格納部と、

前記第 1 の機器へデータを送信する第 2 の送信部と、

前記第 1 の機器から送信されたデータを受信する第 2 の受信部と、

前記第 1 の公開鍵証明書を検証する第 2 の証明書検証部と、

第 2 の鍵と第 2 の鍵を暗号化した前記第 2 の暗号化鍵を生成する第 2 の暗号化鍵生成部と、

前記第 1 の暗号化鍵から復号化し、前記第 1 の鍵を出力する第 2 の暗号化鍵復号部と、

前記第 1 の鍵と前記第 2 の鍵に基づき共有鍵を生成する前記共有鍵生成部と、

前記共有鍵を格納する前記共有鍵格納部とを含むこと

を特徴とする認証鍵共有システム。

【請求項 7】

コンテンツ送信機器とコンテンツ受信機器を備え、前記コンテンツ送信機器と前記コンテンツ受信機器との間で鍵配送を行い、共有した鍵を用いて暗号化通信を行う暗号通信システムにおけるコンテンツ送信機器であって、

第 1 の公開鍵証明書と第 1 のコンテンツデータを格納する第 1 のデータ格納部と、

前記コンテンツ受信機器へデータを送信する第 1 の送信部と、

前記コンテンツ受信機器から送信されたデータを受信する第 1 の受信部と、

前記コンテンツ受信機器に対する第 2 の公開鍵証明書を検証する第 1 の証明書検証部と、

第 1 の鍵と第 1 の鍵を暗号化した第 1 の暗号化鍵を生成する第 1 の暗号化鍵生成部と、
前記コンテンツ受信機器から送信される第 2 の暗号化鍵を復号化し、復号化した結果を第 2 の鍵として出力する第 1 の暗号化鍵復号部と、

前記第 1 の鍵と前記第 2 の鍵に基づき共有鍵を生成する共有鍵生成部と、

前記共有鍵を格納する共有鍵格納部と、

前記共有鍵の一部または全部を用いて、前記第 1 のコンテンツデータを共通鍵暗号を用いて暗号化した第 1 の暗号化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて第 1 のハッシュ値を生成する第 1 の暗号化部とを備えること

を特徴とするコンテンツ送信機器。

【請求項 8】

前記第 1 の暗号化鍵は、鍵カプセル化メカニズムを用いて生成すること
を特徴とする請求項 7 記載のコンテンツ送信機器。

【請求項 9】

前記共有鍵生成部は、前記第 1 の鍵と前記第 2 の鍵の排他的論理和を前記共有鍵として出力すること

を特徴とする請求項 7 または請求項 8 記載のコンテンツ送信機器。

【請求項 10】

前記共有鍵生成部は、前記第 1 の鍵と前記第 2 の鍵をビット連結したものをハッシュ関数を用いて計算したハッシュ値を前記共有鍵として出力すること

を特徴とする請求項 7 または請求項 8 記載のコンテンツ送信機器。

【請求項 11】

コンテンツ送信機器とコンテンツ受信機器を備え、前記コンテンツ送信機器と前記コンテンツ受信機器との間で鍵配送を行い、共有した鍵を用いて暗号化通信を行う暗号通信システムにおけるコンテンツ受信機器であって、

第 2 の公開鍵証明書と第 2 のコンテンツデータを格納する第 2 のデータ格納部と、

前記コンテンツ送信機器へデータを送信する第 2 の送信部と、

前記コンテンツ送信機器から送信されたデータを受信する第 2 の受信部と、

前記コンテンツ送信機器に対する第 1 の公開鍵証明書を検証する第 2 の証明書検証部と

、
第 2 の鍵と第 2 の鍵を暗号化した第 2 の暗号化鍵を生成する第 2 の暗号化鍵生成部と、
前記コンテンツ送信機器から送信された第 1 の暗号化鍵を復号化し、復号化した結果を第 1 の鍵として出力する第 2 の暗号化鍵復号部と、

前記第 1 の鍵と第 2 の鍵に基づき共有鍵を生成する共有鍵生成部と、

前記共有鍵を格納する共有鍵格納部と、

前記コンテンツ送信機器から送信された第 1 の暗号化コンテンツデータを復号化し、第 1 の復号コンテンツデータを取得し、前記第 1 の復号コンテンツデータに対して、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて第 2 のハッシュ値を生成し、第 1 のハッシュ値と比較する第 1 の復号化部とを備えること

を特徴とするコンテンツ受信機器。

【請求項 12】

前記第 2 の暗号化鍵は、鍵カプセル化メカニズムを用いて生成すること

を特徴とする請求項 11 記載のコンテンツ受信機器。

【請求項 13】

前記共有鍵生成部は、前記第 1 の鍵と前記第 2 の鍵の排他的論理和を前記共有鍵として出力すること

を特徴とする請求項 11 または請求項 12 記載のコンテンツ受信機器。

【請求項 14】

前記共有鍵生成部は、前記第 1 の鍵と前記第 2 の鍵をビット連結したものをハッシュ関数を用いて計算したハッシュ値を前記共有鍵として出力すること

を特徴とする請求項 11 または請求項 12 記載のコンテンツ受信機器。

【請求項 15】

第 1 の機器と第 2 の機器を備え、前記第 1 の機器と前記第 2 の機器との間で鍵配送を行い、共有した鍵を用いて前記第 1 の機器から前記第 2 の機器へコンテンツデータを送信する暗号通信方法であって、

第 1 の公開鍵証明書と第 1 のコンテンツデータを格納する第 1 のデータ格納ステップと

、
前記第 2 の機器へデータを送信する第 1 の送信ステップと、

前記第 2 の機器から送信されたデータを受信する第 1 の受信ステップと、

第 2 の公開鍵証明書を検証する第 1 の証明書検証ステップと、

第 1 の鍵と第 1 の鍵を暗号化した第 1 の暗号化鍵を生成する第 1 の暗号化鍵生成ステッ

ブと、

第2の暗号化鍵から復号化し、復号化した結果を第2の鍵として出力する第1の暗号化鍵復号ステップと、

前記第1の鍵と前記第2の鍵に基づき共有鍵を生成する共有鍵生成ステップと、

前記共有鍵を格納する共有鍵格納ステップと、

前記共有鍵の一部または全部を用いて、前記第1のコンテンツデータを共通鍵暗号を用いて暗号化した第1の暗号化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて第1のハッシュ値を生成する第1の暗号化ステップとを前記第1の機器に実行させ、

前記第2の公開鍵証明書と前記第2のコンテンツデータを格納する第2のデータ格納ステップと、

前記第1の機器へデータを送信する第2の送信ステップと、

前記第1の機器から送信されたデータを受信する第2の受信ステップと、

前記第1の公開鍵証明書を検証する第2の証明書検証ステップと、

第2の鍵と第2の鍵を暗号化した前記第2の暗号化鍵を生成する第2の暗号化鍵生成ステップと、

前記第1の暗号化鍵から復号化し、復号化した結果を前記第1の鍵として出力する第2の暗号化鍵復号ステップと、

前記第1の鍵と前記第2の鍵に基づき共有鍵を生成する前記共有鍵生成ステップと、

前記共有鍵を格納する前記共有鍵格納ステップと、

前記第1の暗号化コンテンツデータを復号化し、第1の復号コンテンツデータを取得し、前記第1の復号コンテンツデータに対して、前記共有鍵の一部または全部と前記鍵付ハッシュ関数を用いて第2のハッシュ値を生成し、前記第1のハッシュ値と比較する第1の復号化ステップとを前記第2の機器に実行させること

を特徴とする暗号通信方法。

【請求項16】

第1の機器はさらに、第2の暗号化コンテンツデータを復号化し、第2の復号コンテンツデータを取得し、前記第2の復号コンテンツデータに対して、前記共有鍵の一部または全部と前記鍵付ハッシュ関数を用いて第3のハッシュ値を生成し、第4のハッシュ値と比較する第2の復号化ステップを含み、

第2の機器はさらに、前記共有鍵の一部または全部を用いて、前記第2のコンテンツデータを暗号化した前記第2の暗号化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて前記第4のハッシュ値を生成する第2の暗号化ステップを含むこと

を特徴とする請求項15記載の暗号通信方法。

【請求項17】

前記第1の暗号化鍵及び前記第2の暗号化鍵は、鍵カプセル化メカニズムを用いて生成すること

を特徴とする請求項15または請求項16記載の暗号通信方法。

【請求項18】

コンテンツ送信機器とコンテンツ受信機器を備え、前記コンテンツ送信機器と前記コンテンツ受信機器との間で鍵配送を行い、共有した鍵を用いて暗号化通信を行う暗号通信システムにおけるコンテンツ送信機器で実行されるプログラムであって、

第1の公開鍵証明書と第1のコンテンツデータを格納する第1のデータ格納ステップと

、前記コンテンツ受信機器へデータを送信する第1の送信ステップと、

前記コンテンツ受信機器から送信されたデータを受信する第1の受信ステップと、

前記コンテンツ受信機器に対する第2の公開鍵証明書を検証する第1の証明書検証ステップと、

第1の鍵と第1の鍵を暗号化した第1の暗号化鍵を生成する第1の暗号化鍵生成ステッ

プと、

前記コンテンツ受信機器から送信される第2の暗号化鍵を復号化し、復号化した結果を第2の鍵として出力する第1の暗号化鍵復号ステップと、

前記第1の鍵と前記第2の鍵に基づき共有鍵を生成する共有鍵生成ステップと、

前記共有鍵を格納する共有鍵格納ステップと、

前記共有鍵の一部または全部を用いて、前記第1のコンテンツデータを共通鍵暗号を用いて暗号化した第1の暗号化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて第1のハッシュ値を生成する第1の暗号化ステップとをコンテンツ送信機器に実行させること

を特徴とするプログラム。

【請求項19】

コンテンツ送信機器とコンテンツ受信機器を備え、前記コンテンツ送信機器と前記コンテンツ受信機器との間で鍵配送を行い、共有した鍵を用いて暗号化通信を行う暗号通信システムにおけるコンテンツ受信機器で実行されるプログラムであって、

第2の公開鍵証明書と第2のコンテンツデータを格納する第2のデータ格納ステップと

前記コンテンツ送信機器へデータを送信する第2の送信ステップと、

前記コンテンツ送信機器から送信されたデータを受信する第2の受信ステップと、

前記コンテンツ送信機器に対する前記第1の公開鍵証明書を検証する第2の証明書検証ステップと、

第2の鍵と第2の鍵を暗号化した第2の暗号化鍵を生成する第2の暗号化鍵生成ステップと、

前記コンテンツ送信機器から送信された第1の暗号化鍵を復号化し、復号化した結果を前記第1の鍵として出力する第2の暗号化鍵復号ステップと、

前記第1の鍵と前記第2の鍵に基づき共有鍵を生成する共有鍵生成ステップと、

前記共有鍵を格納する共有鍵格納ステップと、

前記コンテンツ送信機器から送信された第1の暗号化コンテンツデータを復号化し、第1の復号コンテンツデータを取得し、前記第1の復号コンテンツデータに対して、前記共有鍵の一部または全部と前記鍵付ハッシュ関数を用いて第2のハッシュ値を生成し、前記第1のハッシュ値と比較する第1の復号化ステップとをコンテンツ受信機器に実行させること

を特徴とするプログラム。

【請求項20】

請求項18または請求項19に記載のプログラムを記録した媒体。

【書類名】明細書

【発明の名称】暗号通信システム、認証鍵共有システム、コンテンツ送信機器、コンテンツ受信機器及び暗号通信方法

【技術分野】

【0001】

本発明は、情報セキュリティ技術としての暗号技術に関する。

【背景技術】

【0002】

近年、家庭用電化製品、携帯電話などの間でネットワークを介した通信を行う機会が増加している。例えば、AV機器では、コンテンツの著作権保護のために、機器同士で、また、携帯電話では通信内容の漏洩を防ぐため、認証鍵共有を行った後に、共有した鍵を用いて暗号化した通信を行うことがある。ここで、認証鍵共有とは、機器同士などで、通信相手の機器が正しく作られた機器であるかを、相互認証により確認し、それと同時に鍵を共有するものである。以下は、AV機器同士をIEEE1394で接続したときに使用される、DTCP (Digital Transmission Content Protection) と呼ばれる著作権保護規格で規定されている認証鍵共有方法を示している (非特許文献1参照)。この方法は、認証方式に楕円DSA署名を用いたチャレンジ・レスポンス認証を使用し、鍵共有方式に楕円DH鍵共有を使用している。チャレンジ・レスポンス認証、楕円DSA署名及び楕円DH鍵共有については、非特許文献2が詳しい。図4でその処理を示す。

【0003】

(従来例1: 認証鍵共有)

以下では従来例1である認証鍵共有方法の処理を示す。以下の認証鍵共有方法ではユーザAとBとの間で相互認証及び鍵共有を行う。なお、ユーザAは公開鍵証明書Cert_Aとそれに対応する秘密鍵KSA及びセンタ公開鍵KPCを保持する。ユーザBは公開鍵証明書Cert_Bとそれに対応する秘密鍵KSB及びセンタ公開鍵KPCを保持する。

【0004】

ステップS201: ユーザBはまず、ユーザAに自身の公開鍵証明書Cert_BとチャレンジデータcBを送る。ここで、Cert_Bは、Bの公開鍵KPBとそのセンタ署名SCB=Sig(KSC, KPB)である。ここで、Sig(KSC, KPB)はセンタ秘密鍵KSCを用いて作成した公開鍵KPBに対する署名データである。

【0005】

ステップS202: 次にユーザAは、Cert_B、cBを受信し、Cert_Bに含まれる公開鍵KPBとその署名SCBに対して、センタ公開鍵KPCを用いて、署名SCBが公開鍵KPBに対する正しいセンタ署名であるかを検証する。その結果、正しいセンタ署名でなければ処理を終了させる。正しいセンタ署名であれば、次のステップS203へ進む。

【0006】

ステップS203: ユーザAは、自身の公開鍵証明書Cert_AとチャレンジデータcAをユーザBに送信する。ここで、Cert_Aは、Aの公開鍵KPAとそのセンタ署名SCA=Sig(KSC, KPA)である。

【0007】

ステップS204: ユーザBは、Cert_A、cAを受信し、Cert_Aに含まれる公開鍵KPBとその署名SCAに対して、センタ公開鍵KPCを用いて、署名SCAが公開鍵KPBに対する正しいセンタ署名であるかを検証する。その結果、正しいセンタ署名でなければ処理を終了させる。正しいセンタ署名であれば、次のステップS205へ進む。

【0008】

ステップS205: ユーザAは、乱数kAを発生させ、楕円DH鍵共有の第1フェーズの値 $kA * G$ を計算する。ここで、Gは、ベース点であり、 $kA * G$ は楕円曲線上の点G

を kA 回加算することにより得られる楕円曲線上の点を表す。

【0009】

ステップ S206: ユーザ A は、 cB と $kA * G$ の連結に対して、秘密鍵 KSA を用いて、署名 $SA = \text{Sig}(KSA, cB || kA * G)$ を作成する。ここで、 $x || y$ は x と y の連結を示す。

【0010】

ステップ S207: ユーザ A は、 cB 、 $kA * G$ 及び SA をユーザ B に送信する。

【0011】

ステップ S208: ユーザ B は、 cB 、 $kA * G$ 及び SA を受信し、ユーザ A の公開鍵 KPA を用いて、署名 SA が cB と $kA * G$ の連結に対する正しい署名であるか検証する。正しくなければ、システムを終了させる。それ以外は次のステップ S209 へ進む。

【0012】

ステップ S209: ユーザ B は、乱数 kB を発生させ、楕円 DH 鍵共有の第 1 フェーズの値 $kB * G$ を計算する。

【0013】

ステップ S210: ユーザ B は、 cA と $kB * G$ の連結に対して、秘密鍵 KSB を用いて、署名 $SB = \text{Sig}(KSB, cA || kB * G)$ を作成する。

【0014】

ステップ S211: ユーザ B は、 cA 、 $kB * G$ 及び SB をユーザ A に送信する。

【0015】

ステップ S212: ユーザ A は、 cA 、 $kB * G$ 及び SB を受信し、ユーザ B の公開鍵 KPB を用いて、署名 SB が cA と $kB * G$ の連結に対する正しい署名であるか検証する。正しくなければ、システムを終了させる。それ以外は次のステップ S213 へ進む。

【0016】

ステップ S213: ユーザ B は、 $kA * G$ と kB を用いて、 $kB * (kA * G)$ を計算し、それを共有鍵とする。

【0017】

ステップ S214: ユーザ A は、 $kB * G$ と kA を用いて、 $kA * (kB * G)$ を計算し、それを共有鍵とし、終了する。

【0018】

また、最近、公開鍵暗号においては、数学的な問題が求解困難である場合に、秘密鍵を持たないユーザが暗号文を解読することができないという安全性の証明をすることが多くなっている。この安全性の証明により、公開鍵暗号の安全性の保証をする。このような証明を「安全性証明」と呼ぶ。例えば、楕円曲線を利用する ECIES 暗号は、 $a * G$ と $b * G$ から、 $a * (b * G)$ を求める Diffie-Hellman 問題と呼ばれる問題が求解困難である場合に、安全であることが証明されている。ECIES 暗号及びその証明については、非特許文献 6 が詳しい。

【非特許文献 1】DTCP Specification の White paper
<URL: <http://www.dtcp.com/spec.html>>

【非特許文献 2】岡本龍明、山本博資、”現代暗号”、産業図書 (1997 年)

【非特許文献 3】Victor Shoup, “A proposal for an ISO standard for public key encryption (version 2.1)”, [online]、2001 年 12 月 20 日、[2002 年 9 月 29 日検索]、インターネット<URL: http://shoup.net/papers/iso-2_1.pdf>

【非特許文献 4】Tatsuaki Okamoto, “Generic constructions for constructing IND-CCA2 public-key encryption in the random oracle model”, [online]、The 5th Workshop on Elliptic Curve Cryptography (ECC 2001)、

2001年10月30日、[2002年9月29日検索]、インターネット<URL : <http://www.cacr.math.uwaterloo.ca/conferences/2001/ecc/okamoto.ppt>>

【非特許文献5】Neal Koblitz, "Algebraic Aspects of Cryptography", Algorithms and Computation in Mathematics Vol. 3, pp. 132-133, Springer-Verlag, 1998.

【非特許文献6】M. Bellare and P. Rogaway, "Minimizing the use of random oracles in authenticated encryption schemes. In Proceedings of PKCS' 97, 1997.

【発明の開示】

【発明が解決しようとする課題】

【0019】

しかしながら、DTCPの認証鍵共有方法では安全性の証明がなされておらず、安全性に不安がある。

【0020】

本発明は、安全性証明がされている暗号方式を利用することで、安全性が保証される認証鍵共有システムを提供することを目的とする。

【課題を解決するための手段】

【0021】

上記目的を達成するために、請求項1における発明は、第1の機器と第2の機器を備え、前記第1の機器と前記第2の機器との間で鍵配送を行い、共有した鍵を用いて前記第1の機器から前記第2の機器へコンテンツデータを送信する暗号通信システムであって、前記第1の機器は、第1の公開鍵証明書と第1のコンテンツデータを格納する第1のデータ格納部と、前記第2の機器へデータを送信する第1の送信部と、前記第2の機器から送信されたデータを受信する第1の受信部と、第2の公開鍵証明書を検証する第1の証明書検証部と、第1の鍵と第1の鍵を暗号化した第1の暗号化鍵を生成する第1の暗号化鍵生成部と、第2の暗号化鍵から復号化し、復号化した結果を第2の鍵として出力する第1の暗号化鍵復号部と、前記第1の鍵と前記第2の鍵に基づき共有鍵を生成する共有鍵生成部と、前記共有鍵を格納する共有鍵格納部と、前記共有鍵の一部または全部を用いて、前記第1のコンテンツデータを共通鍵暗号を用いて暗号化した第1の暗号化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて第1のハッシュ値を生成する第1の暗号化部とを含み、前記第2の機器は、前記第2の公開鍵証明書と前記第2のコンテンツデータを格納する第2のデータ格納部と、前記第1の機器へデータを送信する第2の送信部と、前記第1の機器から送信されたデータを受信する第2の受信部と、前記第1の公開鍵証明書を検証する第2の証明書検証部と、第2の鍵と第2の鍵を暗号化した前記第2の暗号化鍵を生成する第2の暗号化鍵生成部と、前記第1の暗号化鍵から復号化し、復号化した結果を前記第1の鍵として出力する第2の暗号化鍵復号部と、前記第1の鍵と前記第2の鍵に基づき共有鍵を生成する前記共有鍵生成部と、前記共有鍵を格納する前記共有鍵格納部と、前記第1の暗号化コンテンツデータを復号化し、第1の復号コンテンツデータを取得し、前記第1の復号コンテンツデータに対して、前記共有鍵の一部または全部と前記鍵付ハッシュ関数を用いて第2のハッシュ値を生成し、前記第1のハッシュ値と比較する第1の復号化部とを含むことを特徴とする。

【0022】

請求項2における発明は、第1の機器はさらに、第2の暗号化コンテンツデータを復号化し、第2の復号コンテンツデータを取得し、前記第2の復号コンテンツデータに対して、前記共有鍵の一部または全部と前記鍵付ハッシュ関数を用いて第3のハッシュ値を生成し、第4のハッシュ値と比較する第2の復号化部を含み、第2の機器はさらに、前記共有鍵の一部または全部を用いて、前記第2のコンテンツデータを暗号化した前記第2の暗号

化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて前記第 4 のハッシュ値を生成する第 2 の暗号化部を含むことを特徴とする。

【0023】

請求項 3 における発明は、前記第 1 の暗号化鍵及び前記第 2 の暗号化鍵は、鍵カプセル化メカニズムを用いて生成することを特徴とする。

【0024】

請求項 4 における発明は、前記共有鍵生成部は、前記第 1 の鍵と前記第 2 の鍵の排他的論理和を前記共有鍵として出力することを特徴とする。

【0025】

請求項 5 における発明は、前記共有鍵生成部は、前記第 1 の鍵と前記第 2 の鍵をビット連結したものをハッシュ関数を用いて計算したハッシュ値を前記共有鍵として出力することを特徴とする。

【0026】

請求項 6 における発明は、第 1 の機器と第 2 の機器を備え、前記第 1 の機器と前記第 2 の機器との間で鍵配送を行う認証鍵共有システムであって、前記第 1 の機器は、第 1 の公開鍵証明書と第 1 のコンテンツデータを格納する第 1 のデータ格納部と、前記第 2 の機器へデータを送信する第 1 の送信部と、前記第 2 の機器から送信されたデータを受信する第 1 の受信部と、第 2 の公開鍵証明書を検証する第 1 の証明書検証部と、鍵カプセル化メカニズムを用いて第 1 の鍵と第 1 の鍵を暗号化した第 1 の暗号化鍵を生成する第 1 の暗号化鍵生成部と、第 2 の暗号化鍵から復号化し、第 2 の鍵を出力する第 1 の暗号化鍵復号部と、前記第 1 の鍵と前記第 2 の鍵に基づき共有鍵を生成する共有鍵生成部と、前記共有鍵を格納する共有鍵格納部とを含み、前記第 2 の機器は、前記第 2 の公開鍵証明書と前記第 2 のコンテンツデータを格納する第 2 のデータ格納部と、前記第 1 の機器へデータを送信する第 2 の送信部と、前記第 1 の機器から送信されたデータを受信する第 2 の受信部と、前記第 1 の公開鍵証明書を検証する第 2 の証明書検証部と、第 2 の鍵と第 2 の鍵を暗号化した前記第 2 の暗号化鍵を生成する第 2 の暗号化鍵生成部と、前記第 1 の暗号化鍵から復号化し、前記第 1 の鍵を出力する第 2 の暗号化鍵復号部と、前記第 1 の鍵と前記第 2 の鍵に基づき共有鍵を生成する前記共有鍵生成部と、前記共有鍵を格納する前記共有鍵格納部とを含むことを特徴とする。

【0027】

請求項 7 における発明は、コンテンツ送信機器とコンテンツ受信機器を備え、前記コンテンツ送信機器と前記コンテンツ受信機器との間で鍵配送を行い、共有した鍵を用いて暗号化通信を行う暗号通信システムにおけるコンテンツ送信機器であって、第 1 の公開鍵証明書と第 1 のコンテンツデータを格納する第 1 のデータ格納部と、前記コンテンツ受信機器へデータを送信する第 1 の送信部と、前記コンテンツ受信機器から送信されたデータを受信する第 1 の受信部と、前記コンテンツ受信機器に対する第 2 の公開鍵証明書を検証する第 1 の証明書検証部と、第 1 の鍵と第 1 の鍵を暗号化した第 1 の暗号化鍵を生成する第 1 の暗号化鍵生成部と、前記コンテンツ受信機器から送信される第 2 の暗号化鍵を復号化し、復号化した結果を第 2 の鍵として出力する第 1 の暗号化鍵復号部と、前記第 1 の鍵と前記第 2 の鍵に基づき共有鍵を生成する共有鍵生成部と、前記共有鍵を格納する共有鍵格納部と、前記共有鍵の一部または全部を用いて、前記第 1 のコンテンツデータを共通鍵暗号を用いて暗号化した第 1 の暗号化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて第 1 のハッシュ値を生成する第 1 の暗号化部とを備えることを特徴とする。

【0028】

請求項 8 における発明は、前記第 1 の暗号化鍵は、鍵カプセル化メカニズムを用いて生成することを特徴とする。

【0029】

請求項 9 における発明は、前記共有鍵生成部は、前記第 1 の鍵と前記第 2 の鍵の排他的論理和を前記共有鍵として出力することを特徴とする。

【0030】

請求項10における発明は、前記共有鍵生成部は、前記第1の鍵と前記第2の鍵をビット連結したものをハッシュ関数を用いて計算したハッシュ値を前記共有鍵として出力することを特徴とする。

【0031】

請求項11における発明は、コンテンツ送信機器とコンテンツ受信機器を備え、前記コンテンツ送信機器と前記コンテンツ受信機器との間で鍵配送を行い、共有した鍵を用いて暗号化通信を行う暗号通信システムにおけるコンテンツ受信機器であって、第2の公開鍵証明書と第2のコンテンツデータを格納する第2のデータ格納部と、前記コンテンツ送信機器へデータを送信する第2の送信部と、前記コンテンツ送信機器から送信されたデータを受信する第2の受信部と、前記コンテンツ送信機器に対する前記第1の公開鍵証明書を検証する第2の証明書検証部と、第2の鍵と第2の鍵を暗号化した第2の暗号化鍵を生成する第2の暗号化鍵生成部と、前記コンテンツ送信機器から送信された第1の暗号化鍵を復号化し、復号化した結果を第1の鍵として出力する第2の暗号化鍵復号部と、前記第1の鍵と第2の鍵に基づき共有鍵を生成する共有鍵生成部と、前記共有鍵を格納する共有鍵格納部と、前記コンテンツ送信機器から送信された第1の暗号化コンテンツデータを復号化し、第1の復号コンテンツデータを取得し、前記第1の復号コンテンツデータに対して、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて第2のハッシュ値を生成し、第1のハッシュ値と比較する第1の復号化部とを備えることを特徴とする。

【0032】

請求項12における発明は、前記第2の暗号化鍵は、鍵カプセル化メカニズムを用いて生成することを特徴とする。

【0033】

請求項13における発明は、前記共有鍵生成部は、前記第1の鍵と前記第2の鍵の排他的論理和を前記共有鍵として出力することを特徴とする。

【0034】

請求項14における発明は、前記共有鍵生成部は、前記第1の鍵と前記第2の鍵をビット連結したものをハッシュ関数を用いて計算したハッシュ値を前記共有鍵として出力することを特徴とする。

【0035】

請求項15における発明は、第1の機器と第2の機器を備え、前記第1の機器と前記第2の機器との間で鍵配送を行い、共有した鍵を用いて前記第1の機器から前記第2の機器へコンテンツデータを送信する暗号通信方法であって、第1の公開鍵証明書と第1のコンテンツデータを格納する第1のデータ格納ステップと、前記第2の機器へデータを送信する第1の送信ステップと、前記第2の機器から送信されたデータを受信する第1の受信ステップと、第2の公開鍵証明書を検証する第1の証明書検証ステップと、第1の鍵と第1の鍵を暗号化した第1の暗号化鍵を生成する第1の暗号化鍵生成ステップと、第2の暗号化鍵から復号化し、復号化した結果を第2の鍵として出力する第1の暗号化鍵復号ステップと、前記第1の鍵と前記第2の鍵に基づき共有鍵を生成する共有鍵生成ステップと、前記共有鍵を格納する共有鍵格納ステップと、前記共有鍵の一部または全部を用いて、前記第1のコンテンツデータを共通鍵暗号を用いて暗号化した第1の暗号化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて第1のハッシュ値を生成する第1の暗号化ステップとを前記第1の機器に実行させ、前記第2の公開鍵証明書と前記第2のコンテンツデータを格納する第2のデータ格納ステップと、前記第1の機器へデータを送信する第2の送信ステップと、前記第1の機器から送信されたデータを受信する第2の受信ステップと、前記第1の公開鍵証明書を検証する第2の証明書検証ステップと、第2の鍵と第2の鍵を暗号化した前記第2の暗号化鍵を生成する第2の暗号化鍵生成ステップと、前記第1の暗号化鍵から復号化し、復号化した結果を前記第1の鍵として出力する第2の暗号化鍵復号ステップと、前記共有鍵生成ステップと、前記共有鍵格納ステップと、前記第1の暗号化コンテンツデータを復号化し、第1の復号コンテンツデータを取得

し、前記第1の復号コンテンツデータに対して、前記共有鍵の一部または全部と前記鍵付ハッシュ関数を用いて第2のハッシュ値を生成し、前記第1のハッシュ値と比較する第1の復号化ステップとを前記第2の機器に実行させることを特徴とする。

【0036】

請求項16における発明は、第1の機器はさらに、第2の暗号化コンテンツデータを復号化し、第2の復号コンテンツデータを取得し、前記第2の復号コンテンツデータに対して、前記共有鍵の一部または全部と前記鍵付ハッシュ関数を用いて第3のハッシュ値を生成し、第4のハッシュ値と比較する第2の復号化ステップを含み、第2の機器はさらに、前記共有鍵の一部または全部を用いて、前記第2のコンテンツデータを暗号化した前記第2の暗号化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて前記第4のハッシュ値を生成する第2の暗号化ステップを含むことを特徴とする。

【0037】

請求項17における発明は、前記第1の暗号化鍵及び前記第2の暗号化鍵は、鍵カプセル化メカニズムを用いて生成することを特徴とする。

【0038】

請求項18における発明は、コンテンツ送信機器とコンテンツ受信機器を備え、前記コンテンツ送信機器と前記コンテンツ受信機器との間で鍵配送を行い、共有した鍵を用いて暗号化通信を行う暗号通信システムにおけるコンテンツ送信機器で実行されるプログラムであって、第1の公開鍵証明書と第1のコンテンツデータを格納する第1のデータ格納ステップと、前記コンテンツ受信機器へデータを送信する第1の送信ステップと、前記コンテンツ受信機器から送信されたデータを受信する第1の受信ステップと、前記コンテンツ受信機器に対する第2の公開鍵証明書を検証する第1の証明書検証ステップと、第1の鍵と第1の鍵を暗号化した第1の暗号化鍵を生成する第1の暗号化鍵生成ステップと、前記コンテンツ受信機器から送信される第2の暗号化鍵を復号化し、復号化した結果を第2の鍵として出力する第1の暗号化鍵復号ステップと、前記第1の鍵と前記第2の鍵に基づき共有鍵を生成する共有鍵生成ステップと、前記共有鍵を格納する共有鍵格納ステップと、前記共有鍵の一部または全部を用いて、前記第1のコンテンツデータを共通鍵暗号を用いて暗号化した第1の暗号化コンテンツデータと、前記共有鍵の一部または全部と鍵付ハッシュ関数を用いて第1のハッシュ値を生成する第1の暗号化ステップとをコンテンツ送信機器に実行させることを特徴とする。

【0039】

請求項19における発明は、コンテンツ送信機器とコンテンツ受信機器を備え、前記コンテンツ送信機器と前記コンテンツ受信機器との間で鍵配送を行い、共有した鍵を用いて暗号化通信を行う暗号通信システムにおけるコンテンツ受信機器で実行されるプログラムであって、第2の公開鍵証明書と第2のコンテンツデータを格納する第2のデータ格納ステップと、前記コンテンツ送信機器へデータを送信する第2の送信ステップと、前記コンテンツ送信機器から送信されたデータを受信する第2の受信ステップと、前記コンテンツ送信機器に対する前記第1の公開鍵証明書を検証する第2の証明書検証ステップと、第2の鍵と第2の鍵を暗号化した第2の暗号化鍵を生成する第2の暗号化鍵生成ステップと、前記コンテンツ送信機器から送信された第1の暗号化鍵を復号化し、復号化した結果を前記第1の鍵として出力する第2の暗号化鍵復号ステップと、前記第1の鍵と前記第2の鍵に基づき共有鍵を生成する共有鍵生成ステップと、前記共有鍵を格納する共有鍵格納ステップと、前記コンテンツ送信機器から送信された第1の暗号化コンテンツデータを復号化し、第1の復号コンテンツデータを取得し、前記第1の復号コンテンツデータに対して、前記共有鍵の一部または全部と前記鍵付ハッシュ関数を用いて第2のハッシュ値を生成し、前記第1のハッシュ値と比較する第1の復号化ステップとをコンテンツ受信機器に実行させることを特徴とする。

【0040】

請求項20における発明は、請求項18または19に記載のプログラムを記録した媒体

【発明の効果】

【0041】

これらの構成によると、鍵カプセル化メカニズム、共通鍵暗号と鍵付ハッシュ関数を用いることにより、安全性を保証でき、双方向で暗号化鍵を送りあうことにより、認証鍵共有を実現できるため、その価値は大きい。

【発明を実施するための最良の形態】

【0042】

(実施の形態1)

本発明にかかる実施の形態1としての暗号通信システム1000について説明する。

【0043】

図1は、実施の形態1における暗号通信システム1000の構成を示す図である。本システムは、機器A1100、機器B1200から構成される。

【0044】

<機器A1100の構成>

機器A1100は、データを保持するデータ格納部1101と、データを送信する送信部1102と、情報を受信する受信部1103と、証明書を検証する証明書検証部1104と、秘密鍵KSAを格納する秘密鍵格納部1105と、暗号化鍵を生成する暗号化鍵生成部1106と、暗号化鍵を復号する暗号化鍵復号部1107と、共有鍵を生成する共有鍵生成部1108と、共有鍵を格納する共有鍵格納部1109と、コンテンツデータを暗号化する暗号化部1110と、コンテンツデータを復号化する復号化部1111とを備える。

【0045】

データ格納部1101は、証明書Cert__A、センタ署名検証鍵KPC及びコンテンツデータDAを保持する。ここで、Cert__Aは公開鍵KPAとそのセンタ署名SKPA=Sig(KSC, KPA)からなる。なお、Cert__Aに他データ例えば、ID情報が含まれてもよいし、センタ署名SKPAがKPAと他のデータ、例えば、ID情報との連結に対する署名であってもよい。KSCはセンタ署名検証鍵KPCに対するセンタ署名生成鍵であり、Sig(KSC, KPA)はセンタ署名生成鍵KSCを用いたKPAの署名を意味する。なお、証明書Cert__A及びセンタ署名検証鍵KPCは、予め証明書センタが作成して配布されているものとする。ここで使用する署名方式は、例えばRSA署名、楕円DSA署名である。署名方式については、非特許文献2が詳しい。

【0046】

送信部1102は、機器B1200へデータを送信する。

【0047】

受信部1103は、機器B1200から送信されたデータを受信する。

【0048】

証明書検証部1104は、機器B1200の公開鍵KPBの証明書Cert__Bに含まれている公開鍵KPBとそのセンタ署名SKPBに対し、データ格納部1101に格納されているセンタ署名検証鍵KPCを用いて、センタ署名SKPBが公開鍵KPBの正しい署名であるか署名検証する。

【0049】

秘密鍵格納部1105は、秘密鍵KSAを秘密に格納する。

【0050】

暗号化鍵生成部1106は、鍵KAとその暗号化鍵KEMAを生成する。この鍵KA及び暗号化鍵KEMAは、鍵配送方式の一種である鍵カプセル化メカニズム(Key Encapsulation Mechanisms)と呼ばれる方式を用いて作成する。鍵カプセル化メカニズムについては、非特許文献3が詳しい。鍵カプセル化メカニズムについては、機器A1100内の各部の説明をした後で詳しく述べる。

【0051】

暗号化鍵復号部1107は、機器B1200より送信される暗号化鍵KEMBを復号化

し、鍵KBを出力する。暗号化鍵KEMBは、先に述べた鍵カプセル化メカニズムにより、作成されている。そのため、ここでの復号化も、鍵カプセル化メカニズムの復号化を用いて行う。

【0052】

共有鍵生成部1108は、鍵KA及び鍵KBより、共通鍵暗号用共有鍵KSとハッシュ用共有鍵KHを生成する。具体的には、例えば、鍵KAとKBの排他的論理和を取り、その一部を共有鍵暗号用共有鍵KSとし、それ以外の部分をハッシュ用共有鍵KHとする。この方法は、鍵KAとKBの両方の一部または全部の情報がKS、KHに含まれるものであればよい。

【0053】

共有鍵格納部1109は、共通鍵暗号用共有鍵KSとハッシュ用共有鍵KHを格納する。

【0054】

データ暗号化部1110は、コンテンツデータDAを共通鍵暗号用共有鍵KSを用いて暗号化し、Enc(KS, DA)を作成し、ハッシュ用共有鍵KHを用いて、ハッシュ値Hash(KH, DA)。ここで、Enc(KS, DA)は鍵KSを用いてDAを共通鍵暗号で暗号化した暗号文であり、Hash(KH, DA)は鍵KHを用いて、鍵付ハッシュ関数で計算したDAのハッシュ値を意味する。共通鍵暗号は例えばDES暗号やAES暗号である。また、Hash(KH, DA)は、Hash(KH, DA) = SHA1(KH || DA)としてもよい。ここで、SHA1(x)は、xのSHA1ハッシュ関数値であり、||は連結を示す。共通鍵暗号及び鍵付ハッシュ関数については、非特許文献2が詳しい。

【0055】

データ復号化部1111は、コンテンツデータDBの暗号文CDB = Enc(KS, DB)を復号化して、データDB'を取得し、データDB'のハッシュ値HDB' = Hash(KH, DB')を計算し、HDBと比較する。

【0056】

(鍵カプセル化メカニズム)

以下で鍵カプセル化メカニズムについて詳しく述べる。

【0057】

鍵カプセル化メカニズムは、簡単に説明すると、公開鍵暗号を用いて送信装置と受信装置の間で共有鍵を配送するアルゴリズムであり、送信側が、公開鍵暗号化アルゴリズムEに受信者の公開鍵pkを入力して暗号文Cと共有鍵Kを生成し、暗号文Cを受信側に伝送する。そして、受信側が、公開鍵復号アルゴリズムDに、秘密鍵skと暗号文Cを入力して送信側と同じ共有鍵Kを求める方式である。

【0058】

鍵カプセル化メカニズムの目的は、鍵カプセル化メカニズムで共有鍵Kを送信装置と受信装置で共有することにより、その後、送信装置から受信装置へ通信される通信内容データを、共有鍵Kを用いて共通鍵暗号で暗号化することにある。ここで、送信者から受信者に一方的に情報の送信が行われていながら、送信者が作為的に共有鍵を作成できず、送信者による不正が抑制されている点が従来の鍵配送方式にない特徴である。

【0059】

このような鍵カプセル化メカニズムとして、PSEC-KEMと呼ばれるアルゴリズムが開示されている(例えば、非特許文献4参照)。以下に、この非特許文献4に記載されているPSEC-KEMアルゴリズムについて説明する。

【0060】

(1) PSEC-KEMのシステムパラメータ

PSEC-KEMは、以下のシステムパラメータを持つ。

【0061】

・楕円曲線: E

- ・楕円曲線上の位数 n の点: P
- ・ハッシュ関数: G, H

なお、楕円曲線、位数及びハッシュ関数については、非特許文献 2 に詳細が記述されているので、ここでは説明を省略する。

【0062】

(2) PSEC-KEMの公開鍵と秘密鍵

- ・ランダムに Z_n の要素 x を選び、 $W = x * P$ を生成する。

【0063】

ここで、 Z_n は、 $\{0, 1, \dots, n-1\}$ からなる集合であり、 $x * P$ は、楕円曲線上の点 P を x 回加算することにより得られる楕円曲線上の点を表す。なお、楕円曲線上の点の加算方法については、非特許文献 2 に記述されている。

【0064】

- ・公開鍵 p_k を (E, P, W, n) とし、秘密鍵 s_k を x とする。

【0065】

(3) PSEC-KEMの暗号化

暗号化時には、以下に述べる公開鍵暗号化アルゴリズム $KemE$ に公開鍵 p_k を入力して共有鍵 K と暗号文 C を出力する。以下に公開鍵暗号化アルゴリズム $KemE$ について説明する。

【0066】

- ・ Z_n の要素 s をランダムに生成する。

【0067】

・ $G(s)$ を生成し、 $G(s)$ を $G(s) = a || K$ と分割する。ここで、 $||$ はビット結合を表し、 $G(s)$ を $G(s) = a || K$ と分割するとは、 $G(s)$ の上位複数ビットを a とし、残りのビットを K とすることを表す。

【0068】

- ・ $R = a * P$, $Q = a * W$ を生成する。

【0069】

・ $v = s \text{ xor } H(R || Q)$ を生成する。ここで、 xor は排他的論理和演算を表す。

【0070】

- ・共有鍵 K と暗号文 $C = (R, v)$ を出力する。

【0071】

(4) PSEC-KEMの復号化

復号化時には、以下に述べる公開鍵復号アルゴリズム $KemD$ に暗号文 $C = (R, v)$ と公開鍵 p_k と秘密鍵 s_k を入力して共有鍵 K を出力する。以下に復号アルゴリズム $KemD$ について説明する。

【0072】

- ・ $Q = x * R$ を生成する。

【0073】

- ・ $s' = v \text{ xor } H(R || Q)$ を生成する。

【0074】

- ・ $G(s')$ を生成し、 $G(s')$ を $G(s') = a || K$ と分割する。

【0075】

- ・ $R = a * P$ が成立するかどうかチェックする。成立すれば共有鍵 K を出力する。

【0076】

この PSEC-KEM アルゴリズムを、送信装置と受信装置の間で暗号化通信を行う暗号システムに応用した場合、まず、送信装置は、通信先受信装置の公開鍵 p_k を取得し、取得した公開鍵 p_k を前述の公開鍵暗号化アルゴリズム $KemE$ に入力して共有鍵 K と暗号文 C を導出して、暗号文 C を受信装置へ送信する。そして、受信装置は、送信装置から暗号文 C を受信し、受信した暗号文 C と自身が有する公開鍵 p_k ・秘密鍵 s_k を前述の公

開鍵復号アルゴリズム $KemD$ に入力して、送信装置が導出したものと等しい共有鍵 K を導出する。

【0077】

以下に、このことを詳細に説明する。

【0078】

今、 $PSEC-KEM$ アルゴリズムは、ハッシュ関数 H の入力を $(a * P || a * W)$ としており、公開鍵暗号化アルゴリズム $KemE$ で、ランダムに生成した要素 s に $H(a * P || a * W)$ の値を作用させて v を生成する。そして、公開鍵復号アルゴリズム $KemD$ では、 $R = a * P$ から秘密鍵 $s_k (= x)$ を用いて $Q = x * R = x * (a * P) = a * (x * P) = a * W$ を求めることができるので、 $v \text{ xor } H(a * P || a * W)$ を計算することにより、公開鍵暗号化アルゴリズム $KemE$ において生成されたランダムな要素 s を求めることができる。従って、公開鍵暗号化アルゴリズム $KemE$ と公開鍵復号アルゴリズム $KemD$ は、ハッシュ関数 G に同じ s の値を入力することができ、同じ共有鍵 K を導出することができる。この結果、秘密鍵 s_k を有する受信装置は、送信装置が導出したものと同じ共有鍵 K を導出できることになる。

【0079】

一方で、秘密鍵 s_k を知らない他の受信装置は、たとえ公開鍵 p_k を取得して暗号文 C を受信したとしても、秘密鍵 $s_k (= x)$ を知らないので $R = a * P$ から $Q = a * W (= (a * x) * P)$ を計算できず、送信装置が導出したものと同じ共有鍵 K を導出できない。なぜならば、秘密鍵 s_k を知らない他の受信装置は、公開鍵 p_k しか利用できないので、上記 Q の計算には秘密鍵 $s_k (= x)$ の代わりに公開鍵 p_k の $W = x * P$ を利用することになるが、一般に、 $a * P$ と $W = x * P$ から、 $Q = a * W (= (a * x) * P)$ を求めることは、楕円曲線上の $Diffie-Hellman$ 問題と呼ばれ、 a や x の値を知らない限り計算困難だからである（例えば、非特許文献 5 参照）。

【0080】

すなわち、 $PSEC-KEM$ アルゴリズムは、秘密鍵を用いずに $a * P$ から $a * W$ を計算することが困難な $Diffie-Hellman$ 問題を用いて、最終的に共有鍵 K を導出することにより、秘密鍵を知らなければその共有鍵 K を導出できないようにしている。

【0081】

よって、以上により、送信装置と受信装置とは、共有鍵 K を秘密に共有することができ、この後、秘密鍵暗号を用いて、送信装置から受信装置へ通信される通信内容データを、共有鍵 K を用いて共通鍵暗号で暗号化することができる。

【0082】

上記の $PSEC-KEM$ アルゴリズムは、先に述べた楕円曲線上の $Diffie-Hellman$ 問題が困難であれば、秘密鍵を知らない受信装置は共有鍵 K を得ることができないことが証明されている。このような証明を方式の安全性を証明していることから、「安全性証明」と呼ぶ。 $PSEC-KEM$ の他の KEM アルゴリズム、例えば $RSA-KEM$ （非特許文献 1 参照）なども同様の困難な数学上の問題を根拠として安全性証明されている。

【0083】

<機器 B120 の構成>

機器 B120 は、データを保持するデータ格納部 1201 と、データを送信する送信部 1202 と、情報を受信する受信部 1203 と、証明書を検証する証明書検証部 1204 と、秘密鍵 KS_B を格納する秘密鍵格納部 1205 と、暗号化鍵を生成する暗号化鍵生成部 1206 と、暗号化鍵を復号する暗号化鍵復号部 1207 と、共有鍵を生成する共有鍵生成部 1208 と、共有鍵を格納する共有鍵格納部 1209 と、コンテンツデータを暗号化する暗号化部 1210 と、コンテンツデータを復号化する復号化部 1211 とを備える。

【0084】

データ格納部 1201 は、公開鍵 KPB 、その証明書 $Cert_B$ 、センタ署名検証鍵

KPC及びコンテンツデータDBを保持する。なお、証明書Cert__B及びセンタ署名検証鍵は、予め証明書センタが作成して配布されているものとする。

【0085】

送信部1202は、機器A1100へデータを送信する。

【0086】

受信部1203は、機器A1100から送信されたデータを受信する。

【0087】

証明書検証部1204は、機器B1100の公開鍵KPAの証明書Cert__Aに含まれている公開鍵KPAとそのセンタ署名SKPAに対し、データ格納部1201に格納されているセンタ署名検証鍵KPCを用いて、センタ署名SKPAが公開鍵KPAの正しい署名であるか署名検証する。

【0088】

秘密鍵格納部1205は、秘密鍵KSBを秘密に格納する。

【0089】

暗号化鍵生成部1206は、鍵KBとその暗号化鍵KEMBを生成する。この鍵KB及び暗号化鍵KEMBは、暗号化鍵生成部1106と同様、鍵カプセル化メカニズムを用いて作成する。

【0090】

暗号化鍵復号部1207は、機器A1100から送信される暗号化鍵KEMAを復号化し、鍵KAを出力する。暗号化鍵KEMAは、先に述べた鍵カプセル化メカニズムにより、作成されている。そのため、ここでの復号化も、鍵カプセル化メカニズムの復号化を用いて行う。

【0091】

共有鍵生成部1208は、鍵KA及び鍵KBより、共通鍵暗号用共有鍵KSとハッシュ用共有鍵KHを生成する。具体的には、例えば、鍵KAとKBの排他的論理和を取り、その一部を共有鍵暗号用共有鍵KSとし、それ以外をハッシュ用共有鍵KHとする。この方法は、鍵KAとKBの両方の一部または全部の情報がKS、KHに含まれるものであればよい。

【0092】

共有鍵格納部1209は、共通鍵暗号用共有鍵KSとハッシュ用共有鍵KHを格納する。

【0093】

データ暗号化部1210は、コンテンツデータDBを、共通鍵暗号用共有鍵KSを用いて暗号化し、Enc(KS, DB)を作成し、ハッシュ用共有鍵KHを用いて、ハッシュ値Hash(KH, DB)。ここで、Enc(KS, DB)は鍵KSを用いてDAを共通鍵暗号で暗号化した暗号文であり、Hash(KH, DB)は鍵KHを用いて、鍵付ハッシュ関数で計算したDBのハッシュ値を意味する。共通鍵暗号は例えばDES暗号やAES暗号である。また、Hash(KH, DB)は、Hash(KH, DB) = SHA1(KH || DB)としてもよい。

【0094】

復号化部1211は、コンテンツデータDAの暗号文CDA = Enc(KS, DA)を復号化して、データDA'を取得し、データDA'のハッシュ値HDA' = Hash(KH, DA')を計算し、HDAと比較する。

【0095】

<暗号通信システム100の動作>

暗号通信システムでは、機器A1100と機器B1200とが相互認証を行い、鍵共有を行った後、共有した鍵を用いて機器A1100と機器B1200の間でコンテンツデータを送信し合う。ここで、コンテンツデータとは、例えば、テキストデータ、音楽データ、画像データ、映画コンテンツデータである。以下でその動作を示す(図2及び図3参照)。

【0096】

ステップS101: 機器B1200内の送信部1202は、データ格納部1201に格納されている、証明書Cert__Bを、機器A1100に送信する。

【0097】

ステップS102: 機器A1100内の受信部1103は、証明書Cert__Bを受信する。

【0098】

ステップS103: 機器A1100内の証明書検証部1104は、証明書Cert__Bに含まれる公開鍵KPB及びその署名SKPBに対して、署名SKPBが公開鍵KPBの正しいセンタ署名であるか否かを、データ格納部1101に格納されているセンタ公開鍵KPCを用いて、検証する。正しいセンタ署名でない場合は、システムを終了させる。正しいセンタ署名の場合は、次のステップS104へ進む。

【0099】

ステップS104: 機器A1100内の暗号化鍵生成部1106は、鍵KAと鍵情報KEMAを作成する。

【0100】

ステップS105: 機器A1100内の送信部1102は、データ格納部1101に格納されている、公開鍵KPA及びその証明書Cert__Aと、鍵情報KEMAを機器B1200へ送信する。

【0101】

ステップS106: 機器B1200内の受信部1203は、公開鍵KPA、その証明書Cert__Aと鍵情報KEMAを受信する。

【0102】

ステップS107: 機器B1200内の証明書検証部1204は、証明書Cert__Aに含まれる公開鍵KPA及びその署名SKPAに対して、署名SKPAが公開鍵KPAの正しいセンタ署名であるか否かを、データ格納部1201に格納されているセンタ公開鍵KPCを用いて、検証する。正しいセンタ署名でない場合は、システムを終了させる。正しいセンタ署名の場合は、次のステップS108へ進む。

【0103】

ステップS108: 機器B1200内の暗号化鍵復号部1207は、秘密鍵格納部1205より秘密鍵KSBを取得し、秘密鍵KSBを用いて、鍵情報KEMAより、鍵KAを復号化する。

【0104】

ステップS109: 機器B1200内の暗号化鍵生成部1206は、鍵KBと鍵情報KEMBを作成する。

【0105】

ステップS110: 機器B1200内の送信部1202は、鍵情報KEMBを機器A1100へ送信する。

【0106】

ステップS111: 機器A1100内の受信部1103は、鍵情報KEMBを受信する。

【0107】

ステップS112: 機器A1100内の暗号化鍵復号部1107は、秘密鍵格納部1105より秘密鍵KSAを取得し、秘密鍵KSBを用いて、鍵情報KEMBより、鍵KBを復号化する。

【0108】

ステップS113: 機器B1200内の共有鍵生成部1208は、鍵KBと復号した鍵KAを用いて、共通鍵暗号用共有鍵KSと鍵付ハッシュ用共有鍵KHを計算し、それぞれを共有鍵格納部1209に格納する。

【0109】

ステップS114: 機器A1100内の共有鍵生成部1108は、鍵KAと復号した鍵KBを用いて、共通鍵暗号用共有鍵KSと鍵付ハッシュ用共有鍵KHを計算し、それぞれ

を共有鍵格納部1109に格納する。

【0110】

ステップS115: 機器A1100内の暗号化部1110は、データ格納部1101に格納されているコンテンツデータDAを、共通鍵暗号用共有鍵KSを用いて暗号化して暗号化コンテンツデータCDAを作成する。さらに暗号化部1110は、鍵付ハッシュ用共有鍵KHを用いて、コンテンツデータDAのハッシュ値HDAを計算する。

【0111】

ステップS116: 機器A1100内の送信部1102は、暗号化コンテンツデータCDAとハッシュ値HDAを機器B1200へ送信する。

【0112】

ステップS117: 機器B1200内の受信部1203は、暗号化コンテンツデータCDAを受信する。

【0113】

ステップS118: 機器B1200内の復号化部1211は、暗号化コンテンツデータCDAを復号して復号コンテンツデータDA'を取得する。さらに復号化部1211は、鍵付ハッシュ用共有鍵KHを用いて、復号コンテンツデータDA'のハッシュ値HDA'を計算し、HDAと比較する。HDA≠HDA'であれば、システムを終了させる。それ以外は復号コンテンツデータDA'をデータ格納部1201に格納する。

【0114】

ステップS119: 機器B1200内の暗号化部1210は、データ格納部1201に格納されているコンテンツデータDBを、共通鍵暗号用共有鍵KSを用いて暗号化して暗号化コンテンツデータCDBを作成する。さらに暗号化部1210は、鍵付ハッシュ用共有鍵KHを用いて、コンテンツデータDBのハッシュ値HDBを計算する。

【0115】

ステップS120: 機器B1200内の送信部1202は、暗号化コンテンツデータCDBとハッシュ値HDBを機器A1100へ送信する。

【0116】

ステップS121: 機器A1100内の受信部1103は、暗号化コンテンツデータCDBを受信する。

【0117】

ステップS122: 機器A1100内の復号化部1111は、暗号化コンテンツデータCDBを復号して復号コンテンツデータDB'を取得する。さらに復号化部1111は、鍵付ハッシュ用共有鍵KHを用いて、復号コンテンツデータDB'のハッシュ値HDB'を計算し、HDBと比較する。HDB≠HDB'であれば、システムを終了させる。それ以外は復号コンテンツデータDB'をデータ格納部1101に格納し、終了する。

【0118】

(実施の形態1の効果)

鍵カプセル化メカニズムで共有した鍵を用いて、データに対して、暗号化した暗号化データとそのデータに対する鍵付ハッシュ関数値を送信するような方式であれば、データ暗号化方法として、困難な数学上の問題を根拠にして安全性証明を可能であることが保証されている(非特許文献3参照)。本方式は、同様に、鍵カプセル化メカニズムで共有した鍵を用いて、コンテンツデータに対して、暗号化した暗号化コンテンツデータとそのコンテンツデータに対する鍵付ハッシュ値を送信しているため、同様の安全性が保証できる。また、機器A1100において、正しい秘密鍵KSAを保持していなければ、暗号化鍵KEMBを復号化して鍵KBを取得できないため、機器B1200と共有した共通鍵暗号用共有鍵KS及び鍵付ハッシュ用共有鍵KHを得られない。そのため、ステップS122におけるデータ復号化ができない。また、機器B1200も同様に、正しい秘密鍵KSBを保持していなければ、暗号化鍵KEMAを復号化して鍵KAを取得できないため、機器A1100と共有した共通鍵暗号用共有鍵KS及び鍵付ハッシュ用共有鍵KHを得られない。そのため、ステップS118のデータ復号化ができない。正しく鍵KAまたは、鍵KB

を取得するためには、正しい秘密鍵 KSA または、KSB が必要である。したがって、両方の機器から暗号化鍵 KEMB, KEMA を送りあうことにより、双方向の認証が実現できている。また、当然ながら、共有鍵を共有できているため、認証鍵共有が実現できている。以上より、安全性を保証できる認証鍵共有を実現でき、その価値は大きい。

【0119】

(変形例)

上記に説明した実施の形態は、本発明の実施の一例であり、本発明はこの実施の形態に何ら限定されるものではなく、その旨を逸脱しない範囲において種々なる態様で実施し得るものである。例えば、以下のような場合も本発明に含まれる。

【0120】

(1) 機器 A 1100 及び機器 B 1200 からコンテンツデータを送り合うが、これが一方、例えば機器 A 1100 のみからコンテンツデータを送るとしてもよい。

【0121】

(2) 共有鍵を共有した後、すぐにコンテンツデータを送信しているが、何らかの処理、例えば、機器の機能（音楽視聴機能、映画視聴機能や放送受信機能など）の確認処理が途中に含まれてもよい。

【0122】

(3) データ格納部に公開鍵、証明書及びコンテンツデータが格納されているとしたが、データ格納部が複数あり、これらのデータが別々に格納されているとしてもよい。

【0123】

(4) 送られたコンテンツデータをデータ格納部に格納しているが、コンテンツデータが例えば、画像データであれば、画面に出力、音楽データであれば、スピーカより出力するとしてもよい。

【0124】

(5) 実施の形態 1 では、証明書 Cert_A を公開鍵 KPA とそのセンタ署名 Sig (KSC, KPA) としているが、これに他データ、例えば、ID 情報を付加してもよい。また、センタ署名の対象データである KPA も、KPA と他のデータ、例えば、ID 情報との連結としてもよい。

【0125】

(6) 実施の形態 1 では、共有鍵生成部で生成する共通鍵暗号用共有鍵 KS と鍵付ハッシュ用共有鍵 KH は、鍵 KA と鍵 KB の排他的論理和の一部であるが、これだけには限らない。例えば、鍵 KA と鍵 KB の連結に対するハッシュ関数値の一部としてもよい。

【産業上の利用可能性】**【0126】**

これらの構成によると、鍵カプセル化メカニズム、共通鍵暗号と鍵付ハッシュ関数を用いることにより、安全性を保証でき、双方向で暗号化鍵を送り合うことにより、認証鍵共有を実現でき、例えば、コンテンツデータを送受信する装置における暗号技術として有用である。

【図面の簡単な説明】**【0127】**

【図 1】 本発明に係る 1 個の実施の形態としての暗号通信システム 1000 の構成を示すシステム構成図

【図 2】 暗号通信システム 1000 の動作を示すフローチャート

【図 3】 暗号通信システム 1000 の動作を示すフローチャート

【図 4】 従来例である D T C P の認証鍵共有方法の動作フロー図

【符号の説明】**【0128】**

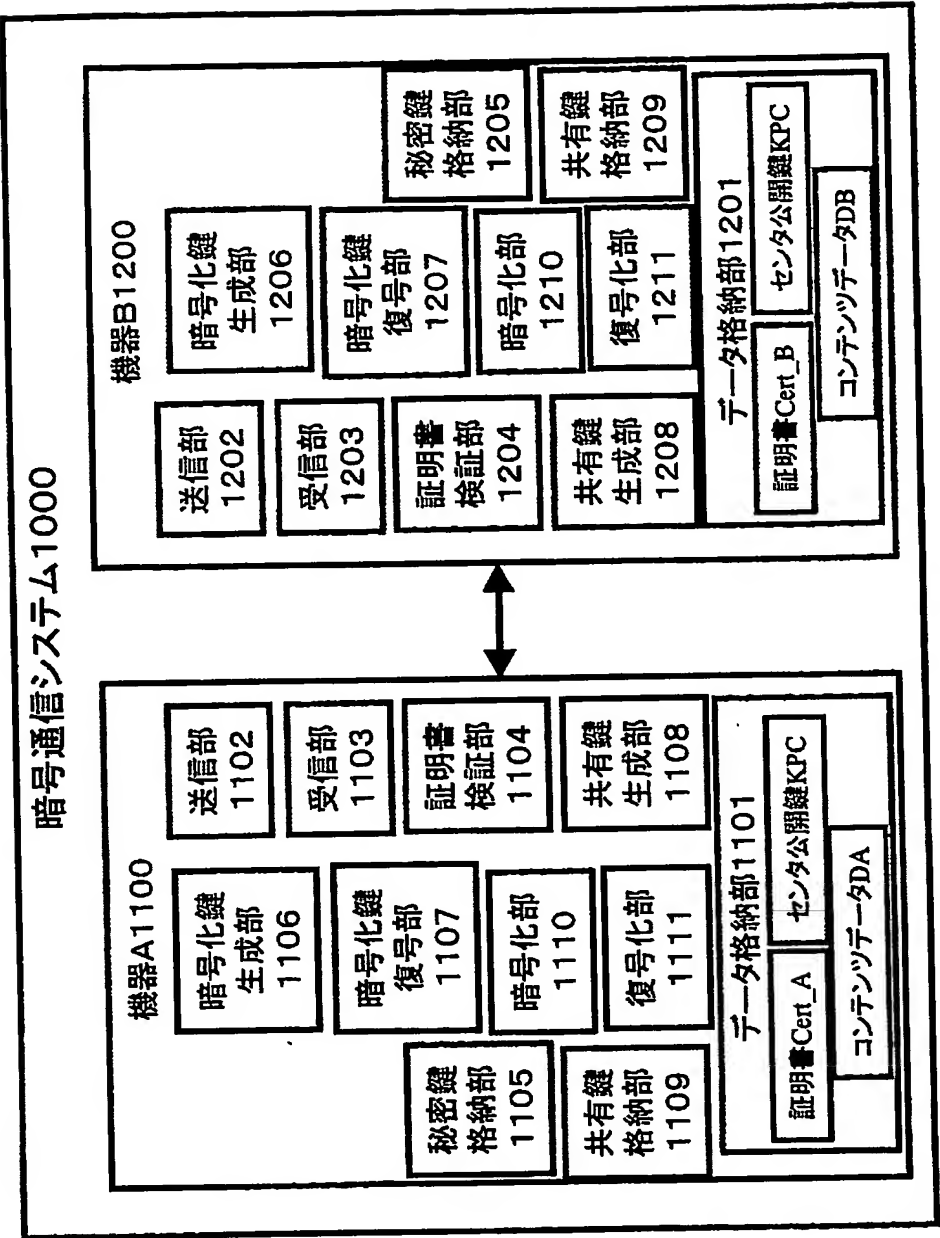
1000 暗号通信システム

1100 機器 A

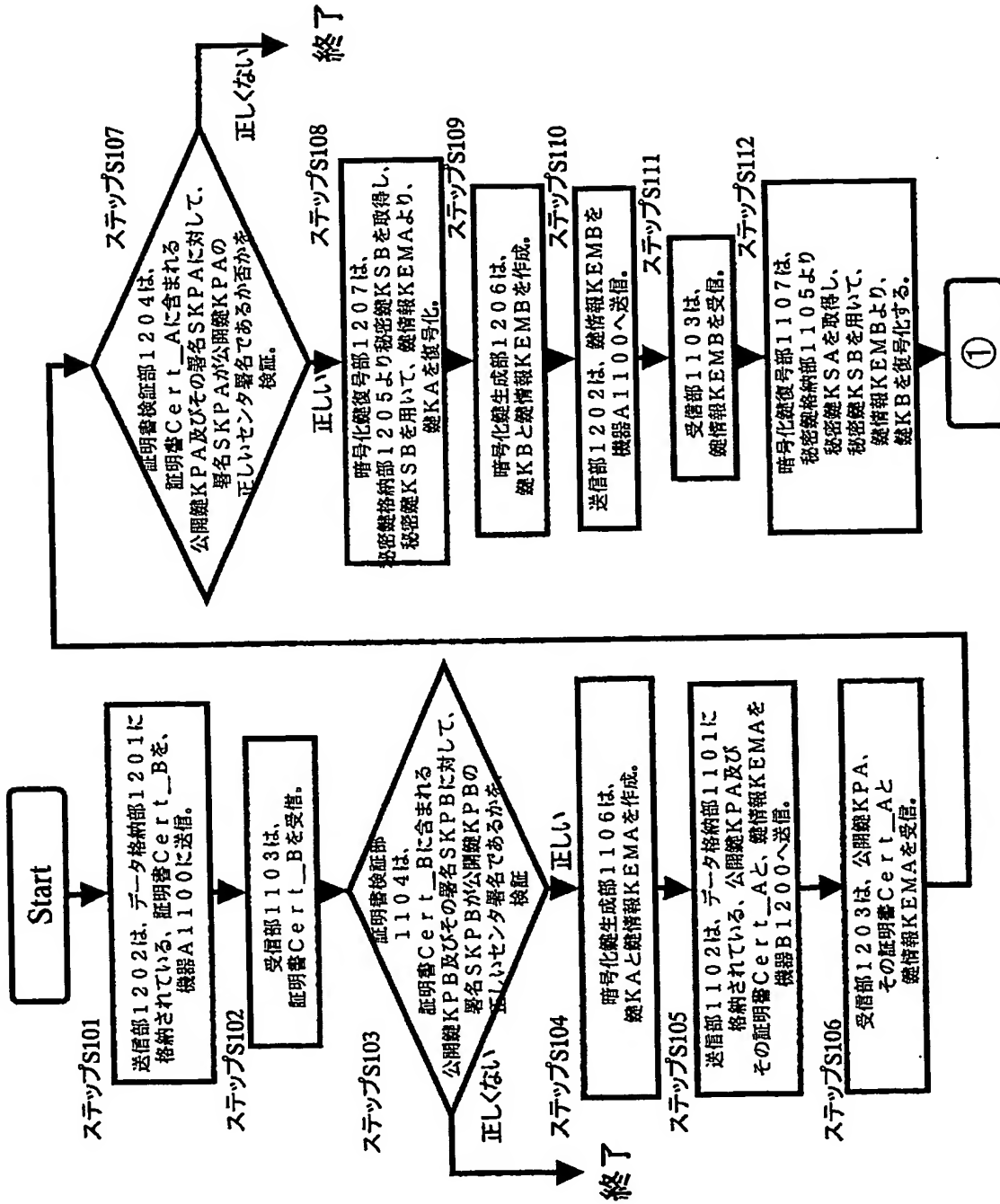
1101, 1201 データ格納部

1 1 0 2, 1 2 0 2	送信部
1 1 0 3, 1 2 0 3	受信部
1 1 0 4, 1 2 0 4	証明書検証部
1 1 0 5, 1 2 0 5	秘密鍵格納部
1 1 0 6, 1 2 0 6	暗号化鍵生成部
1 1 0 7, 1 2 0 7	暗号化鍵復号部
1 1 0 8, 1 2 0 8	共有鍵生成部
1 1 0 9, 1 2 0 9	共有鍵格納部
1 1 1 0, 1 2 1 0	暗号化部
1 1 1 1, 1 2 1 1	復号化部
1 2 0 0	機器 B

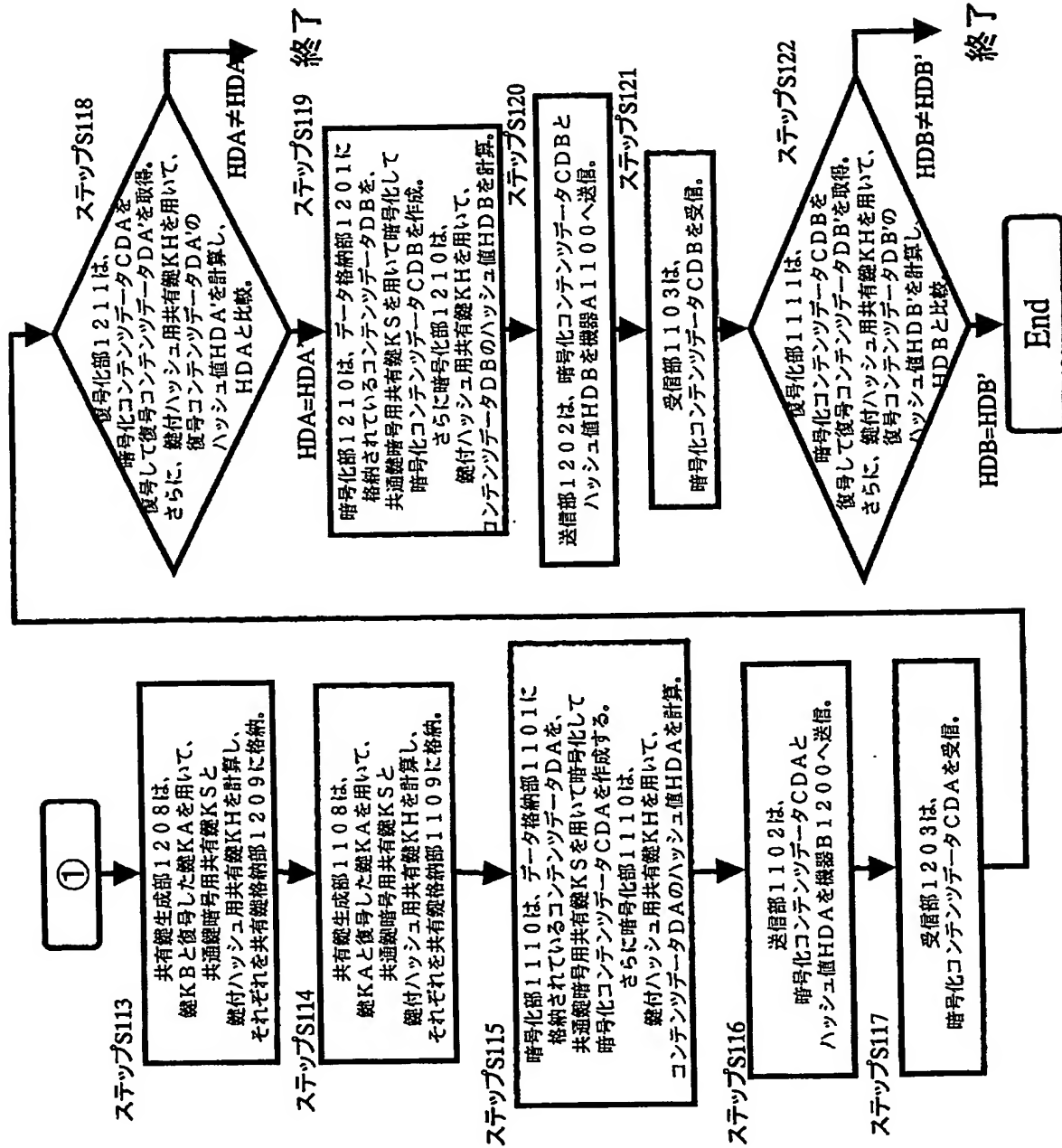
【書類名】 図面
【図 1】



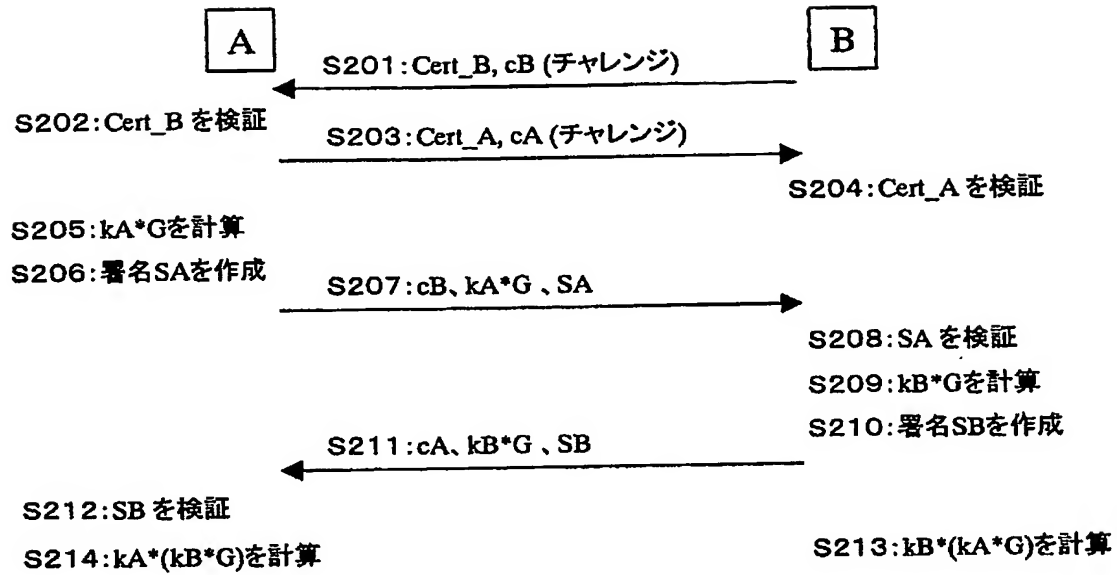
【図2】



【図3】



【図 4】



【書類名】 要約書**【要約】**

【課題】従来の I E E E 1 3 9 4 の著作権保護規格である D T C P の認証鍵共有方法では安全性の証明がなされておらず、安全性に不安が残る。

【解決手段】二者間の通信を以下のように行う。まず、公開鍵証明書認証を相互に行う。次に、鍵カプセル化メカニズムで鍵配送を双方向で行い、2つの共有鍵を得る。さらにその共有鍵の排他的論理和を取ることにより、新たな共有鍵を取得する。その後、新たな共有鍵を共通鍵暗号及び鍵付ハッシュ関数に使用して、二者間でデータ暗号化通信を行う。

【選択図】 図 1

特願 2 0 0 3 - 3 5 6 0 7 3

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☒ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☐ **FADED TEXT OR DRAWING**

☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.